THIS DOCUMENT IS UNCLASSIFIED UNTIL FILLED IN
WHEN FILLED PROTECT AS "FOR OFFICIAL USE ONLY"

NAVY INSPECTOR GENERAL (IG) INFOSEC CHECKLIST

Modified Draft – 6 Sep 01

1. **PURPOSE**. This document assists IG personnel in conducting and documenting the inspection of the Information Assurance (IA) functional area.

2. **REFERENCES**. The primary references used to generate this checklist are:

- DOD Directive 5200.28 - Security Requirements for Automated Information Systems (AIS) of 21 Mar. 88
- DODINST 5200.40 of 30 Dec 97 – DOD Information Technology Security Certification and Accreditation Process (DITSCAP)
- DOD MEMO for Secretaries of 7 Dec 98 – Web Site Administration
- DOD MEMO for Secretaries of 4 Jun 01 – Disposition of Unclassified Hard Drives
- DOD MEMO for Secretaries of 12 Aug 00 – DOD PKI
- DoD Mobile Code Policy – 7 Nov 00
- DoD Draft CPS of 19 Jun 2000- LRA CPS for Class 3 Assurance
- OPNAVINST 5239.1B N6/CMC-C4I of 9 Nov 99 – DON IA Program
- OPNAVINST 2201.2 of 3 Mar 98; Subj: Computer Network Incident Response
- OPNAVINST 2201.3 of 3 Mar 98; COMSEC of USN/USMC Telecom and AIS
- CNO Washington DC 211417Z Oct 98; Subj: IAVA
- CNO Washington DC 172153Z Feb 99; Subj: SysAdmin Training and Certification
- CNO Washington DC 182115Z Feb 99; Subj: SysAdmin Training and Certification
- CNO Washington DC 152300Z Feb 99; Subj: SysAdmin Certification Documentation
- CNO Washington DC 081949Z Sep 99; Subj: Implementation of INFOCON
- CNO Washington DC 211137Z Aug 00; Subj: Navy-Marine Corps Firewall Policy
- SECNAV 5239.3 of 14 Jul 95 - DON INFOSEC Program
- SECNAV 5720.47 of 1 Jul 99 – DON Policy for Content of Publicly Accessible World Wide Web Sites
- Department of the Navy PKI Implementation Plan of 16 Jan 2001
- Naval Information Assurance Program Publications (IA Pubs) 5239 Series
- Novell Netware V5.X Implementation Guide
- UNIX Security Technical Implementation Guide
- SPAWAR Secure Windows NT Installation & Configuration Guide of Jun 98
- Public Law 100-235
- FIWC Vulnerability Analysis and Assistance Program dated 8 march 2001

SUPPLEMENTARY REFERENCES:

- NAVSUP Ltr 5239 63D of 22 Apr 97 - Policy on DOD Electronic Notice and Consent Banner
- NAVSUP Ltr 5239 63D of 7 Oct 99 – NAVSUP Revised Firewall INFOSEC Policy
- NAVSUP Ltr 5230 Ser 63A of 3 Dec 95 – Policy for Use of the Internet
- NAVSUP ltr 5239.0420 065/5016 of 18 Apr 95 – Subj: INFOSEC Guidance for Accessing the Internet
- NAVSUP Ltr 5230 Ser 63A of 1 Aug 96 – WWW Home Page Guidelines
- NAVSUP Ltr 5239 63D of 24 Dec 96 – DON Information Systems Security
- NAVSUP Ltr 5239 63D of 18 Sep 98 – NAVSUP Encryption and PKI Policy for SBU Data
- NAVSUP Ltr 5239 63D of 16 Jan 98 – NAVSUP WWW INFOSEC Policy
- NAVSUP ltr 5239 63 of 17 May 00; Subj: NAVSUP Information Technology Standards and Guidelines
- NAVSUP ltr 5239 63D of 12 Jun 00; Subj: IA Program of NAVSUP
- NAVSUP ltr 5239 63D of 4 Sep 01, Subj: NAVSUP Deployment of DOD/Navy PKI
- NAVSUP Working Notes

3. **OBJECTIVE**.

3.1 Provide a tool to assist in performing IGs in the area of Information Assurance (IA).

3.2 Provide a reminder of the requirements of the above mentioned references.

4. **INSTRUCTIONS**. The questions can be answered with a "yes", "no", or "N/A". A "yes" indicates conformance to the requirement or recommended practice. A "no" indicates a requirement or recommended practice is not being fulfilled. An "N/A" states the requirement or recommended practice is not applicable. Amplifying information may be entered into the comments block available for each question. Generally, no more than 0-2 findings are cited per category. *To further assist you, each category or question has been annotated with a reference.* (CAUTION - this form is locked which allows entry into the preformatted comment and check boxes. Unlocking the form and relocking will cause loss of all entered information.)

CATEGORIES:

A = Accreditation
S = IA Staff
T = Training
G = General
R = Risk Assessment
C = Contingency Plan/Backup
AC = Access Control
P = PC/LAN Security
I = Internet Security
PKI = Public Key Infrastructure
V = Virus Protection
R = Reporting Procedures (IAVAs/Security/Virus Incidents)
CDP = Classified Data Processing

CATEGORY A – ACCREDITATION

(Reference DoD Instruction Number 5200.40 - DITSCAP)

		YES	NO	N/A
1.0	Has a System Security Authorization Agreement (SSAA) been developed per DoDInst 5200.40 - DITSCAP for each system/application under your purview? Comments:	☐	☐	☐
1.1	Does the SSAA identify and account for the current IS environment at the site? Comments:	☐	☐	☐
1.2	Has an effective risk management program been implemented for each system? Comments:	☐	☐	☐
1.3	Do the Risk Assessments (RAs) reflect current system operational environment? Comments:	☐	☐	☐
1.4	Have Security Test and Evaluations (ST&Es) been performed and documented to validate system security posture? Comments:	☐	☐	☐
2.0	If other than the CO, the DAA has been designated in writing as responsible for overall security of connected systems *(Reference Navy IA Pub 5239-01)* Comments:	☐	☐	☐
3.0	Has the Designated Approving Authority (DAA) approved the SSAA for each system? Comments:	☐	☐	☐
4.0	Has the DAA granted Accreditation or Interim Authority to Operate (IATO) for all systems (any information technology that collects, stores, transmits, or processes information)? Comments: Total Systems: _____ Systems Accredited: _____ Systems under IATO: _____	☐	☐	☐
5.0	Is reaccreditation accomplished within three years of the accreditation date? *(Reference DoD Dir 5200.28)* Comments:	☐	☐	☐

CATEGORY S- INFORMATION ASSURANCE (IA) STAFF		YES	NO	N/A
1.0	Has an Information System Security Manager (ISSM) been appointed in writing? *(Reference OPNAVINST 5239.1B)* Comments:	☐	☐	☐
1.1	Is the ISSM a full-time position? If not, why not? *(Reference NAVSUP ltr-12 Jun 00 – IA Program for NAVSUP)* Comments:	☐	☐	☐
1.2	Has the ISSM received formal training related to IA? *(Reference OPNAVINST 5239.1B; IA Pub-5239-04 September 1995)* Comments:	☐	☐	☐
2.0	Has a Network Security Officer (NSO) been appointed in writing? *(Reference IA Pub-5239-08 March 1996)* Comments:	☐	☐	☐
3.0	Have Information Systems Security Officers (ISSOs) been appointed in writing for each system, i.e., email system, all servers? *(Reference OPNAVINST 5239.1B)* Comments:	☐	☐	☐
3.1	Have the ISSOs received formal training on security responsibilities for their assigned system(s)? *(Reference OPNAVINST 5239.1B)* Comments:	☐	☐	☐
3.2	If the ISSO is a contractor or a DOD Service Provider, is the security responsibilities delineated in the contract or Service Level Agreement (SLA)? *(Reference DOD Directive 5200.28)* Comments:	☐	☐	☐
4.0	Have the Firewall Administrators received training? (*Reference NAVSUP Revised Firewall INFOSEC Policy of 7 Oct 99)* Comments:	☐	☐	☐
4.2	Are the firewall audit logs being reviewed? Comments:	☐	☐	☐
	Daily: _____ | Weekly: _____			
5.0	Has a Primary Web Master been appointed in writing? *(Reference SECNAVINST 5720.47)* Comments:	☐	☐	☐

CATEGORY T - TRAINING		YES	NO	N/A
1.0	Has an Information Assurance (IA) Awareness Training Program been established? *(Reference NAVSUP IA Program letter of 12 Jun 00)* Comments:	☐	☐	☐
1.1	Has the DAA been briefed on the IA Training Program? *(Reference OPNAVINST 5239.1B)* Comments:	☐	☐	☐
1.2	Is IA Awareness training being conducted at least annually to all users of information systems as required by *Public Law 100-235?* Comments:	☐	☐	☐
2.0	Does your awareness training address IA responsibilities for users when accessing PC/LAN/Internet? *(Reference NAVSUP IA Program ltr of 12 Jun 00)* Comments:	☐	☐	☐
3.0	Have users been made aware of policy regarding intellectual property and Copyright Laws? *(Reference IA Pub 5239-29 - Controls Over Copyrighted Computer Software)* Comments:	☐	☐	☐
4.0	Are System Administrators trained or in training for the appropriate level of certification training? *(Reference: CNO N6 172153Z Feb 99 & CNO N6 182115Z Feb 99)* Comments:	☐	☐	☐
4.1	Has the completion of system administrator certification training by military personnel and civil service personnel been documented in the local Command Training Records? *(Reference CNO N64 P152300Z Nov 99)* Comments:	☐	☐	☐

CATEGORY G – GENERAL		YES	NO	N/A
1.0	Is there an Information Assurance Program in place? *(Reference IA Pub-5239-01, paragraph 1.3)* Comments:	☐	☐	☐
1.1	Has the DAA been briefed on the IA Program? *(Reference OPNAVINST 5239.1B)* Comments:	☐	☐	☐
2.0	Are IA requirements included in the site's Infrastructure Abbreviated Acquisition Plan (ITIAAP)? *Note: ITIAAP replaces LCM requirements.* Comments:	☐	☐	☐
3.0	Are electronic media and documents containing sensitive data properly labeled per guidance of *IA Pub 5239-01 of May 00?* Comments:	☐	☐	☐
4.0	Are random floor checks conducted to ensure compliance of Navy IA policies and procedures? *(Reference IA Pub 5239-08)* Comments:	☐	☐	☐
5.0	Are new equipment/application plans/purchases made IAW *NAVSUP Information Technology Standards and Guidelines?* Comments:	☐	☐	☐
6.0	Is access to computer centers, server and cable closets limited to personnel who have the need for access? *(Reference Navy IA Pub 5239-01)* Comments:	☐	☐	☐

CATEGORY C - CONTINGENCY PLAN/BACKUP *(Reference IA Pub 5239-01/DODINST 5200.40)*		YES	NO	N/A
1.0	Does the activity have a contingency plan? Comments:	☐	☐	☐
2.0	Are all LAN servers and mini-computer systems being backed-up routinely? Comments:	☐	☐	☐
3.0	Are backup tapes being stored off-site? Comments:	☐	☐	☐
3.1	Is the activity using another activity or contractor for off-site storage? Comments:	☐	☐	☐
3.2	Is a MOA established outlining responsibilities of each party? Comments:	☐	☐	☐
3.3	Is the off-site facility physically secure? Comments:	☐	☐	☐
3.4	Does the off-site facility provide protection from possible fire or water damage? Comments:	☐	☐	☐
3.5	Are procedures in place for retrieving backup tapes, utilizing absolute identification of messenger pickup (photograph or ID badge)? Comments:	☐	☐	☐
4.0	Are backup tapes routinely tested to ensure they are working properly? Comments:	☐	☐	☐
5.0	Are critical systems identified for disaster recovery/contingency planning? *(Reference IA Pub 5239-04 o f Sep 95)* Comments:	☐	☐	☐
6.0	Are various disaster levels covered in the contingency plans? Comments:	☐	☐	☐
7.0	Is the contingency plan tested annually? Comments:	☐	☐	☐

CATEGORY AC - ACCESS CONTROL *(Reference IA Pub-5239-01)*		YES	NO	N/A
1.0	Are background checks accomplished on all personnel prior to allowing system access? Comments:	☐	☐	☐
2.0	Are the access control security features on a system, tested regularly. Comments:	☐	☐	☐
2.1	Eight (8) character alphanumeric passwords? Comments:	☐	☐	☐
2.2	Three (3) invalid attempts, then lockout? Comments:	☐	☐	☐
2.3	Are passwords uniquely identifiable to a single user (no group passwords without appropriate justification)? Comments:	☐	☐	☐
2.4	Are password changes forced at least every six months (180 days)? Comments:	☐	☐	☐

CATEGORY P - PC/LAN SECURITY		YES	NO	N/A
1.0	Are the PCs processing sensitive unclassified data CAP compliant? *(Reference IA Pub 5239-15 of Jan 95)* Comments:	☐	☐	☐
1.1	If not, is there a CAP waiver in place for those PCs that are not single user systems and located in a secure area? Comments:	☐	☐	☐
2.0	Has the SPAWAR Secure Windows NT Installation & Configuration Guide been implemented on those systems running WindowsNT operating systems? Comments:	☐	☐	☐
3.0	Is the proper DOD Monitoring Notice displayed on all AISs? *(Reference OPNAVINST 2201.3 March 1998)* Comments:	☐	☐	☐
3.1	Is periodic notification of the monitoring policy provided to all users. *(Reference OPNAVINST 2201.3)* Comments:	☐	☐	☐
4.0	Is the required Privacy Notice posted on major entry points and/or web site page(s)? *(Reference SECNAVINST 5720.47 - DON Policy for Content of Publicly Accessible WWW Sites of 7/1/99)* Comments:	☐	☐	☐
5.0	Has the applicable standard NAVSUP Novell Netware V5.X Implementation Guide been implemented on those systems using Novell operating systems? *(Reference Novell Netware V5.X Implementation Guide)* Comments:	☐	☐	☐
6.0	Has the applicable UNIX Security Implementation Guide been implemented on those systems using UNIX operating systems? *(Reference UNIX Security Technical Implementation Guide)* Comments:	☐	☐	☐
7.0	Is DAA-approved overwriting software used to sanitize hard drives prior to disposal of unclassified systems? *(Reference Memo for Secretaries "Disposition of Unclassfied Hard Drives dated 4 June, 2001)* Comments:	☐	☐	☐
8.0	Is Compact Disk and other optical media destroyed IAW *IA Pub 5239-26?* Comments:	☐	☐	☐

CATEGORY I - INTERNET SECURITY		YES	NO	N/A
1.0	Are ALL servers connected to the Internet compliant with CAP requirements? *(Reference IA Pub 5239-15; NAVSUP WWW policy letter of 16 Jan 98)* Comments:	☐	☐	☐
1.1	If not, is there a CAP waiver in place for those servers? Comments:	☐	☐	☐
2.0	Is Internet access accomplished in accordance with the NAVSUP Policy for Use of the Internet? *(Reference NAVSUPSYSCOM ltr 5230 Ser 63A Dec 8 1995 - Policy for Use of the Internet; CINCLANTFLT Norfolk VA/N6/N631 msg R042354Z May 00-Subj: Internet Policy))* Comments:	☐	☐	☐
3.0	Is Internet access via the NIPRNET/SIPRNET? *(Reference CNO Washington DC 081949Z Sep 99)* Comments:	☐	☐	☐
4.0	Have firewalls been implemented in accordance with the Navy-Marine Corps Firewall Policy to block intrusions? *(Reference CNO Washington DC 211137Z Aug 00)* Comments:	☐	☐	☐
4.1	Are requirements for exceptions to the Navy-Marine Corps Firewall Policy approved by CNO? *(Reference CNO Washington DC 211137Z Aug 00)* Comments:	☐	☐	☐
5.0	Are there vulnerability assessment tools in place for the detection and notification of intrusions into activity servers? *(Reference CNO Washington DC 081949Z Sep 99)* Comments:	☐	☐	☐
5.1	Are intrusions and other incidents reported to FIWC IAW *OPNAVINST 2201.2?* Comments:	☐	☐	☐
6.0	Does the activity have a Modem policy in place? *(Reference CNO Washington DC 081949Z Sep 99 – Attachment – Implementation Guidelines)* Comments:	☐	☐	☐
6.1	Does the activity Modem policy direct that the terminal/laptop must be disconnected from the network prior to and during dial-in operations? *(Reference NAVSUP Dial-in Connections Policy 041428Z Apr 01)* Comments:	☐	☐	☐

CATEGORY I - INTERNET SECURITY (continued)		YES	NO	N/A
7.0	Do owners of your Web sites comply with the DoD/Navy/NAVSUP INFOSEC Web policies/guidance on privacy banner, strong identification/authentication of user if non-public, installation of intrusion detection software, etc? *(Reference DOD Memo of 7 Dec 98 - Web Site Administration; NAVSUP WWW INFOSEC Policy of 16 Jan 98)* Comments:	☐	☐	☐
8.0	Is an On-Line Survey conducted by the Fleet Information Warfare Center annually to identify network vulnerabilities? *(Reference FIWC Vulnerability Analysis and Assistance Program dated 8 march 2001)* Comments:	☐	☐	☐
9.0	Are MOAs negotiated when network connections and firewall services are provided to business partners? *(Reference DODINST 5200.40)* Comments:	☐	☐	☐
9.1	Do these agreements address INFOSEC requirements of applicable references? *(Reference NAVSUP MOA Working Note; DODINST 5200.40)* Comments:	☐	☐	☐
10.0	Are appropriate control measures in place to protect systems from malicious or improper use of mobile code? *(Reference DOD Mobile Code Policy dated 7 Nov 2000)* Comments:	☐	☐	☐

CATEGORY PKI - PUBLIC KEY INFRASTRUCTURE		YES	NO	N/A
1.0	If sensitive but unclassified data is transmitted/processed via the public network, is the data encrypted? *(Reference DOD Memo of 12 Aug 00; Department of the Navy Public Key (PKI) Implementation Plan of 16 Jan 2001)* Comments:	☐	☐	☐
2.0	Are all "non public" web servers using DoD PKI server certificates with SSL enabled (FIPS 140-1 compliant encryption method)? *(Reference DOD Memo of 12 Aug 00, Department of the Navy Public Key (PKI) Implementation Plan of 16 Jan 2001)* Comments:	☐	☐	☐
3.0	Are there plans in place for migration of all "non public" applications (Web or otherwise) to the DoD PKI and use certificates for client authentication when appropriate? *(Reference DOD Memo of 12 Aug 00 – NAVSUP ltr 4 Sep 01 – NAVSUP Deployment of DOD/Navy DOD PKI; NAVSUP INFOSEC Program Office Metric)* Comments:	☐	☐	☐
4.0	Has your DoD Local Registration Authority (LRA) been nominated in writing by your organization and approved by the Navy RA to authenticate DoD PKI subscribers (verify identity and subscriber information)? *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
5.0	Is the LRA trained and a copy of the Certificate of Training maintained on file? *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
6.0	Is there a signed copy of the LRA Certificate Acceptance and Acknowledgement of Responsibilities form maintained on file *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
7.0	Is the LRA's downloaded Personal Identity certificate generated and stored on a FIPS 140-1, level 2 smartcard? (No backup copy authorized) *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐

CATEGORY PKI - PUBLIC KEY INFRASTRUCTURE (continued)	YES	NO	N/A

8.0	Is LRA only issuing certificates to authorized individuals DoD Military, DoD civilians, and approved contractors with a .mil domain? (No organizational certificates are authorized) *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
9.0	Is the LRA maintaining a file of signed subscriber Certificate Acceptance and Acknowledgement of Responsibilities forms? *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
10.0	Has the LRA or Trusted Agent signed a declaration that he/she personally verified the identity of each subscriber? (Same form as above item) *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
11.0	Is subscriber information kept confidential and properly protected and kept in a locked container? *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
12.0	Does the LRA have a Subscriber Identity Certificate in addition to the LRA certificate for use in performing functions not related to those of an LRA *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
13.0	Is all LRA equipment labeled “For Authorized Use Only?" *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
14.0	Is LRA equipment protected from tampering and from unauthorized access while cryptographic module is installed and activated? *(Reference DoD LRA Certificate Practice Statement of 29 June 2000 - Draft)* Comments:	☐	☐	☐
15.0	Is the LRA workstation set up in compliance with the DOD PKI RA/LRA Workstation Security Settings document? *(Reference DOD PKI RA/LRA Workstation Security Settings Document of Mar 2001)* Comments:	☐	☐	☐

CATEGORY V - VIRUS PROTECTION *(Reference IA Pub-5239-01 of May 2000; CNO Washington DC 081949Z Sep 99)*	**YES**	**NO**	**N/A**

1.0	Is there a virus protection program in place at the activity? Comments:	☐	☐	☐
1.1	Is there an effective virus protection TSR program loaded and run on each PC and every SERVER including the mail servers? Comments:	☐	☐	☐
1.2	Are virus signatures kept up-to-date? Comments:	☐	☐	☐
2.0	Is there a content control email software package implemented on your mail servers? *(Reference NAVSUPSYSCOM lyt 5230/069/Nov 17, 1999 Subj: Electronic Mail Monitoring and NAVSUP Guide to MailSweeper Software of April 2000)* Comments:	☐	☐	☐

CATEGORY R - REPORTING PROCEDURES		YES	NO	N/A
1.0	Are all types of successful INFOSEC incidents (virus attacks, penetration attempts, etc.) investigated, documented, and reported to appropriate personnel and organizations? *(Reference OPNAVINST 2201.2 of 3 Mar 98 - Computer Network Incident Response)* Comments:	☐	☐	☐
2.0	Does your activity comply with the Navy Information Assurance Vulnerability Alert (IAVA) Program? *(Reference CNO 211417Z Oct 98 ZYB)* Comments:	☐	☐	☐
2.1	Are any IAVAs being waived at your site? Comments:	☐	☐	☐
3.0	Has an INFOCON Program been established at your site? *(Reference CNO Washington DC 081949Z Sep 99)* Comments:	☐	☐	☐
3.1	Is the activity operating at the NAVSUP-designated INFOCON level? *(Reference Current NAVSUP messages establishing INFOCON level)* Comments:	☐	☐	☐
3.2	Has the activity implemented all countermeasures for the current INFOCON level? *(Reference NAVSUP INFOCON Working Note)* Comments:	☐	☐	☐

CATEGORY CDP - CLASSIFIED DATA PROCESSING		YES	NO	N/A
1.0	Does the activity process classified information? *(NAVSUP metric)* Comments:	☐	☐	☐
2.0	Does the activity have any requirement to access classified/unclassified on same system, i.e., multi-level security? *(NAVSUP metric)* Comments:	☐	☐	☐
3.0	If you transmit classified data via a wide area network, are you connected to the SIPRNET per *NAVSUP subject Working Note?* Comments:	☐	☐	☐